Technical “Small” Cyber Incident Handling Steps

I. Purpose

The State of Montana and its agencies are under constant threat of malware related activity. The Best Practices workgroup was tasked to provide national industry standard practices for Incident Response and Incident Handling of small cyber related incidents. This document is to provide technical best practices on dealing with malware related activity.

II. Policy

The Technical Small Cyber Incident Handling Steps for Small Incidents applies to the following controls found within the Information Security Policy.

a. Information Security Policy
   - Protect
     - 2.9.5.9
   - Detect
     - 3.2.4
   - Respond
     - 4.1

b. Information Security Policy – Appendix A
   - Incident Response (IR)
     - IR-1 – Incident Response Policy and Procedures
     - IR-4 – Incident Handling
   - System and information Integrity (SI)
     - SI-3 – Malicious Code Protection
     - SI-4 – Information System Monitoring

III. Technical Cyber Incident Handling Steps – Small Cyber Incidents

Non-Critical Incidents

1. Perform full scan of device with approved Anti-Virus/Malware software with added Rootkit detection enabled if available. If unavailable, an approved Rootkit scanning tool must be used as these are typically missed by standard AV toolkits. Re-image if infection is found.

2. Review the installed programs including browser plugins, add-ons, extensions, or toolbars for unauthorized or suspicious applications.

3. Run either the ***netstat –b*** command from the command line or use GUI based SysInternals tool TCPView looking for abnormal network connections specific to the alert. This can help to identify the process responsible for the alert.

4. Review of suspicious autoruns, scheduled tasks, and suspicious processes. Verify processes are digitally signed by trusted vendors. Some helpful tools to accomplish this from SysInternals are:
    - Autoruns
    - Process Explorer
    - Process Monitor

5. Review of the Security, Application, and System Event logs for newly installed and/or created processes around the time frame of the alert.

6. Submit suspect file(s) to multiple online malware analysis site(s) such as:
    - https://www.virustotal.com/
    - https://malwr.com/

7. Investigate user browsing activity during the timeframe of the alert.

8. If web traffic alert is a suspected false positive, request a review of URL from Websense and confirm correct security risk categorization.
    - https://csi.websense.com/

9. If unable to find source of suspicious traffic and system continues to trigger alerts for a confirmed security risk site, a re-image of machine is required.

Critical Incidents

1. Immediate removal from the network and re-image the machine.

NOTE: Retrieval of files from any potentially infected device is solely at the agency's risk. In emergency situation, contact the Service Desk at 444-2000.

Incident Categorization

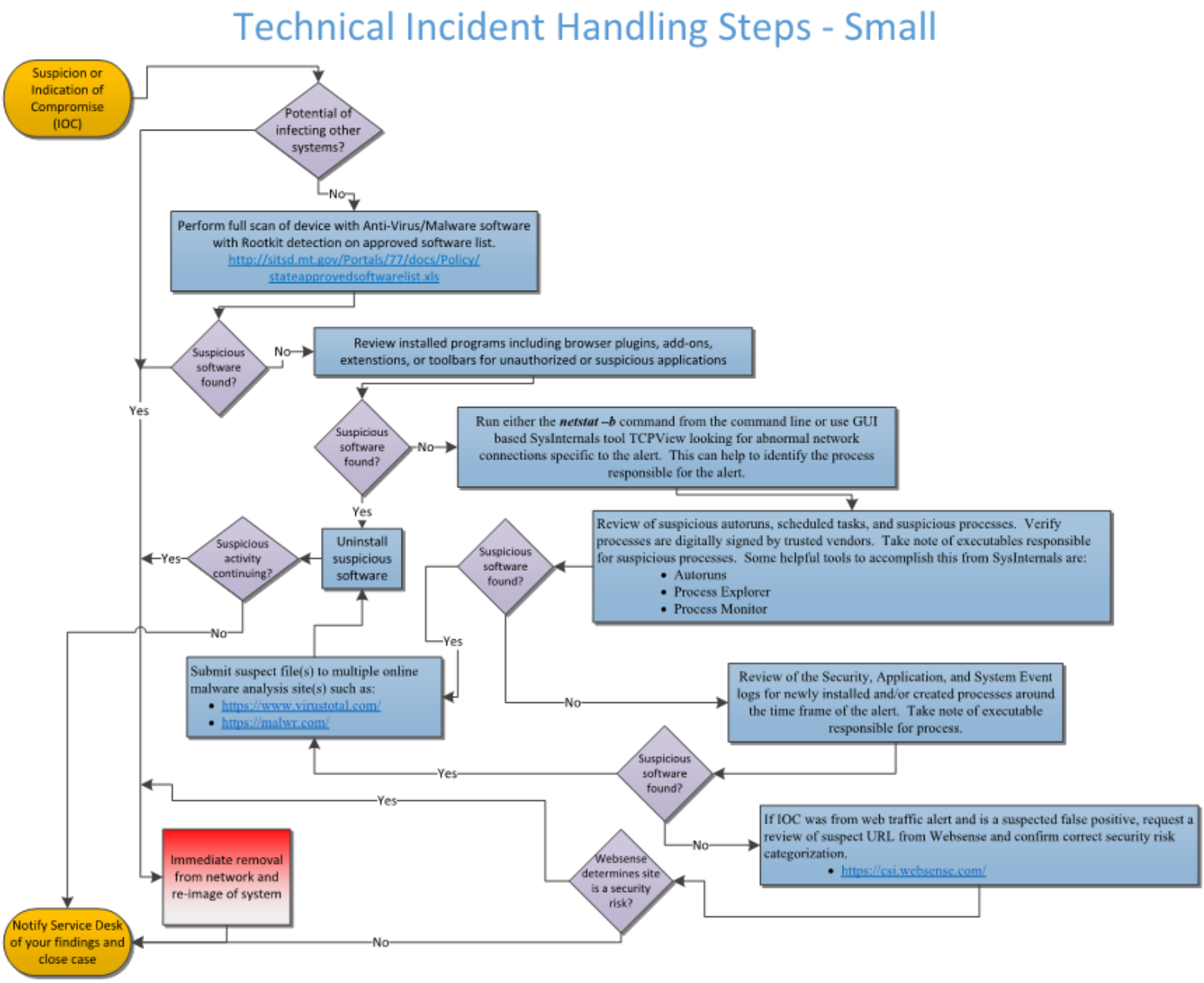
The following chart can be used for reference on what is considered a Critical or Non-Critical incidents pertaining to Splunk/Websense alerts.

Alerts classified as Critical are in RED

Alerts classified as Non-Critical are in Green

Alert Category Name	Hit Threshold (in 1 hour)
Advanced Malware Command and Control Security	1+
Advanced Malware Payloads	1+
Bot Networks	1+ (15 minutes)
Keyloggers Security	1+
Malicious Embedded Link	21+
Malicious Web Sites	20+
Administrator Blocked URL's	10+
Potentially Unwanted Software	10+
Compromised Websites	20+
Custom-Encrypted Uploads	10+
Files Containing Passwords	1+
Malicious Embedded iFrames	21+
Mobile Malware	5+
Phishing and Other Frauds	10+
Potentially Exploited Documents	1+
Spyware Security	1+
Suspicious Embedded Link	21+
Parked Domains	21+

Flowchart - A digital copy of this flowchart can be found on the Best Practices MT-ISAC SharePoint site



IV. Conclusion

This Technical Small Incident Handling document is the result of a multi-agency collaboration as well as has the MT-ISAC Best Practices approval. The representatives from these groups worked well together to endorse the recommendations contained here-in.